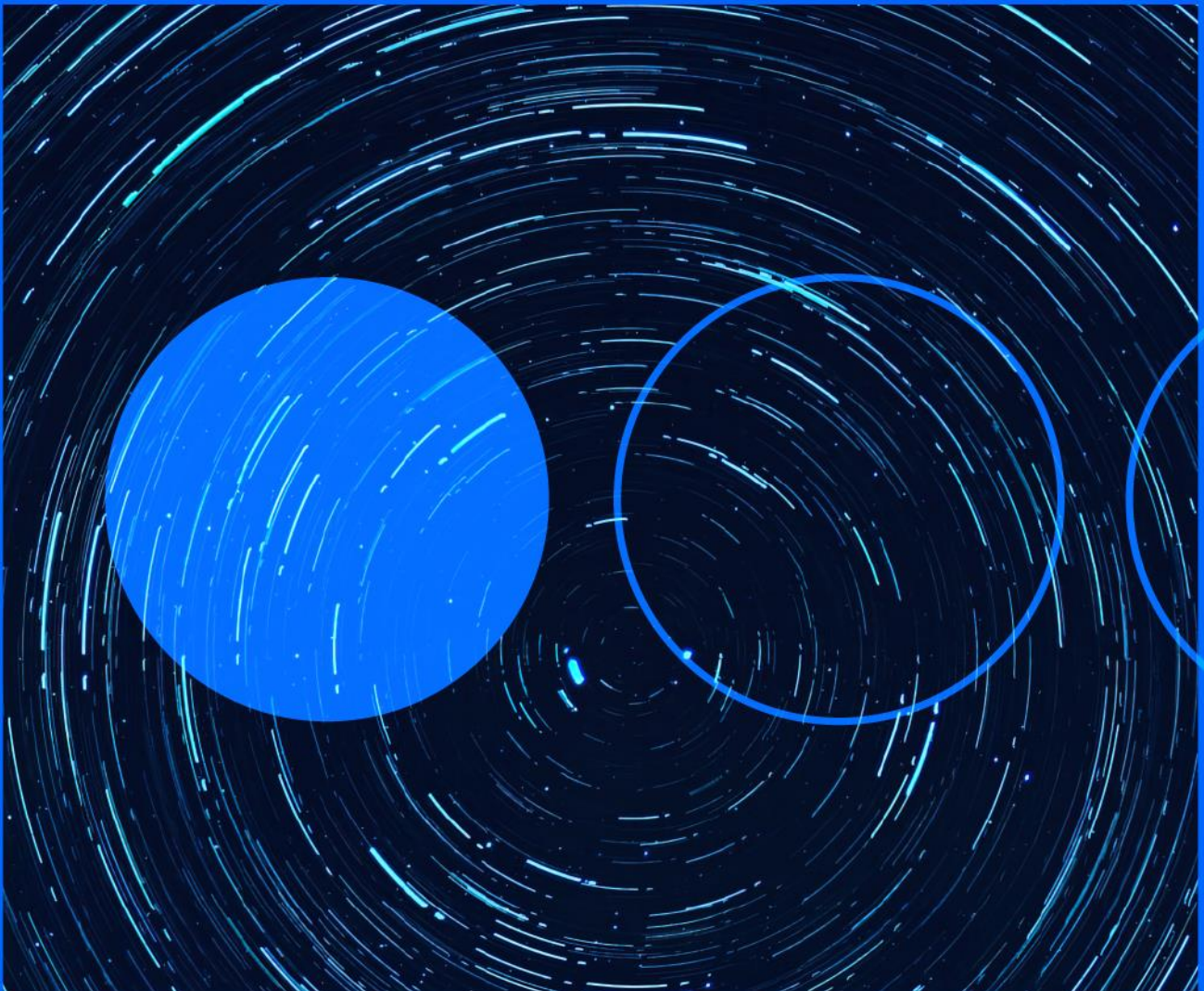







03.03.2023

Cyber threats weekly briefing 2023



Summary of the main attacks and vulnerabilities found by our experts in the last 7 days.

The icons stand for the following concepts:

				
Cyberoperations	Incidents	Malware	Information Leaks	Vulnerabilities



Vulnerabilities in WordPress Houzez

INTERNATIONAL

A security researcher from Patchstack has recently discovered two critical vulnerabilities in Houzez, a WordPress theme and plugin that allows easy and seamless list management for the client. The first vulnerability, identified as [CVE-2023-26540](https://patchstack.com/articles/psa-houzez-theme-unauthenticated-privilege-escalation-vulnerability-exploited-in-the-wild/) and CVSS of 9.8, refers to a configuration bug affecting version 2.7.1 and earlier, and can be exploited remotely without authentication to escalate privileges. On the other hand, the flaw identified as [CVE-2023-26009](https://patchstack.com/articles/psa-houzez-theme-unauthenticated-privilege-escalation-vulnerability-exploited-in-the-wild/) and CVSS 9.8, affects Houzez login in versions 2.6.3 and earlier. In the attacks observed by Patchstack, the threat actors distributed a backdoor capable of executing commands, injecting ads into the website and redirecting to malicious sites, so researchers recommend updating as soon as possible.

URL: <https://patchstack.com/articles/psa-houzez-theme-unauthenticated-privilege-escalation-vulnerability-exploited-in-the-wild/>



Digital Smoke: global investment fraud scam

INTERNATIONAL

The Resecurity team has identified an investment fraud ring, which is said to have operated from 2015 to early 2023. The malicious actors behind this network, which has been named "Digital Smoke", operated by impersonating globally known corporations, such as Verizon, BackRock, Ferrari, Shell, Barclays, among others, in order to get victims, located globally, to invest in fake investment products. Digital Smoke developed a large network of web resources and mobile applications hosted by different hosting providers and jurisdictions. The modus operandi consisted of registering domains similar to the legitimate domains of the spoofed companies, placing the links to register new victims on messaging applications such as WhatsApp and other social networks. Once victims registered on the website or application created by the malicious

actors, they were asked to make a payment for the alleged investment. It should be noted that investigators shared all available information with the Indian Cybercrime Coordination Centre and US authorities in late 2022, with the operation being discontinued in early 2023.

URL: <https://www.resecurity.com/blog/article/resecurity-disrupts-investment-scam-network-digital-smoke>



Aruba fixes six critical vulnerabilities

INTERNATIONAL

Aruba has issued a security advisory reporting six critical vulnerabilities affecting several versions of ArubaOS. The affected products are Aruba Mobility Conductor, Aruba Mobility Controllers and WLAN Gateways and SD-WAN Gateways. On the one hand, the vulnerabilities identified as CVE-2023-22747, CVE-2023-22748, CVE-2023-22749 and CVE-2023-22750, all with CVSSv3 9.8 derive from a command injection flaw. On the other hand, vulnerabilities CVE-2023-22751 and CVE-2023-22752 also both with CVSSv3 9.8, are buffer overflow bugs. These vulnerabilities can be exploited by an unauthenticated attacker to send packets to the PAPI (Aruba Access Point Management Protocol) through UDP port 8211, allowing arbitrary code execution as privileged users on ArubaOS.

URL: <https://www.bleepingcomputer.com/news/security/aruba-networks-fixes-six-critical-vulnerabilities-in-arubaos/>



APT-C-36: new malicious campaign against Ecuador and Colombia

INTERNATIONAL

BlackBerry researchers have published research uncovering a new campaign by APT-C-36, also known as BlindEagle, against geolocated targets in Ecuador and Colombia. In this campaign, malicious actors impersonated Colombia's National Tax and Customs Directorate and Ecuador's Internal Revenue Service in order to launch phishing campaigns targeting key industries in both countries, including the health, financial and governmental sectors. This information follows another discovery in January by [Check Point, which warned](#) of a campaign by the same actor, which they claimed to be interested in monetary gain. However, BlackBerry has indicated that during the most recent incidents the objectives were to steal information and spy on its victims.

URL: <https://blogs.blackberry.com/en/2023/02/blind-eagle-apt-c-36-targets-colombia>



Cryptojacking campaign against Redis databases

INTERNATIONAL

Researchers at Cado Labs have discovered a cryptojacking campaign targeting misconfigured Redis database servers. The campaign is conducted via transfer.sh, an open source file transfer service that has been breached since 2014. The access vector takes place by exploiting an insecure Redis implementation, saving the database in a cron directory that leads to the execution of arbitrary commands. Since the malware's main goal is to mine cryptocurrencies with XMRig, it carries out a number of measures to ensure its effectiveness. Among these, it frees up system memory, removes any cryptominers and installs a network scanner to find other vulnerable Redis servers and spread the infection.

URL: <https://www.cadosecurity.com/redis-miner-leverages-command-line-file-hosting-service/>

About Telefónica Tech

Telefónica Tech is the leading company in digital transformation. The company has a wide range of services and integrated technological solutions for Cybersecurity, Cloud, IoT, Big Data, or Blockchain.

More information

telefonicatech.com



2022 © Telefónica Cybersecurity & Cloud Tech S.L.U. All rights reserved.

The information disclosed in this document is the property of Telefónica Cybersecurity & Cloud Tech S.L.U. ("Telefónica Tech") and/or any other entity within Telefónica Group and/or its licensors. Telefónica Tech and/or any Telefonica Group entity or Telefónica Tech's licensors reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use and sales rights thereto, except to the extent said rights are expressly granted to others. The information in this document is subject to change at any time, without notice.

Neither the whole nor any part of the information contained herein may be copied, distributed, adapted or reproduced in any material form except with the prior written consent of Telefónica Tech.

This document is intended only to assist the reader in the use of the product or service described in the document. In consideration of receipt of this document, the recipient agrees to use such information for its own use and not for other use.

Telefónica Tech shall not be liable for any loss or damage arising out from the use of the any information in this document or any error or omission in such information or any incorrect use of the product or service. The use of the product or service described in this document are regulated in accordance with the terms and conditions accepted by the reader.

Telefónica Tech and its trademarks (or any other trademarks owned by Telefónica Group) are registered service marks.